

EXHIBIT 6



Search

Home Products

Safari
Bookshelf

Authors

Promotions

Chapters &
ArticlesAlliances &
Imprints

Log In | My Account

New Popular Site Help

Home > Articles > Security > Computer Forensics > The Role of Computer Forensics in Stopping Executive Fraud

The Role of Computer Forensics in Stopping Executive Fraud

By Scott Laliberte, Ajay Gupta.

Sample Chapter is provided courtesy of Addison Wesley Professional.

Date: Oct 1, 2004.

 [Save](#)
 [Discuss](#)
 [Print](#)
 [E-mail](#)

Article Information

Contents

1. Introduction: The Whistle-Blower
2. Preparation
3. Evidence Collection and Chain of Custody
4. Drive Imaging
5. Review of the Logical File Structure
6. Review of Unallocated Space and File Slack
7. Smoking Gun
8. Reporting
9. Lessons Learned

Article Description

Virtual evidence is an important part of nearly every modern corporate crime investigation, and proper handling of that evidence can mean the difference between a conviction and a criminal walking free. In this chapter, you'll learn how to properly investigate computer evidence in a corporate environment.

From the Book



Defend I.T.: Security by Example

\$31.49 (Save 10%)



Find the tools and guidance you need for a well-guarded network ►

[Free Tools & Updates](#)
[Security Assessment](#)
[Antivirus](#)

You May Also Like

The Role of Architectural Risk Analysis in Software Security

By Gary McGraw

Mar 3, 2006

Stuart McClure's Daily Security Tips for the Week of November 11th

By Stuart McClure

Nov 8, 2002

Stuart McClure's Daily Security Tips for the Week of November 18th

By Stuart McClure

Nov 15, 2002

See All Related Articles

Search Related Safari

15.5 Review of the Logical File Structure

After imaging the suspect hard drives, we reviewed the logical file structure. To facilitate this process, our team used the EnCase Forensic Edition software. This is a licensed software tool. By using our Linux servers, previously used for hard drive imaging, as file servers (utilizing Samba as the mechanism for file sharing), our Windows-based analysis machines could access the raw data files that contained images of our suspects' hard drives.

With EnCase as our tool, we opened each raw data file and began our analysis. EnCase has the built-in technology to read the file and present the data as if it were actually connected to a hard drive. The view that is represented is similar to what an average Windows-based computer user sees when accessing the Windows Explorer utility (see Figure 15.2).



Figure 15.2 EnCase Logical File Structure Review

A review of logical file structure involves both automated and manual procedures. The computer forensic software being utilized facilitates the automated procedures. By using EnCase, we were able to search through the directories of the suspect's computer system and quickly locate any files that seemed pertinent to our investigation. As a follow-up method, we looked through the directories manually to identify any files that might not have been detected during our automated search with EnCase.

Each file we located that was deemed pertinent to our investigation was copied to the analysis drive, to be included in our computer forensic analysis report. When performing this step it is important to record the logical address of the file. This is the full path name; for example, the full path name of the System32 directory on many Windows NT/2K/XP computers is C:\Winnt\System32.

[Previous Section](#)

6. Review of Unallocated Space and File Slack | [Next Section](#)

Make a New Comment

You must [login](#) in order to post a comment.

Books



Search electronic versions of over 1500 technical books:

[Search](#)

Promotions

Buy One Get One Half Price

Expires: Never

Do You Have an Effective Security Strategy?

Expires: Never

Download Audio Interview with "Exploiting Software" Authors

Expires: Never

[See All Promotions](#)

Most Popular Articles

Secure Coding in C and C++: Strings

By Robert Seacord

Dec 1, 2005

Computer Forensics: Tracking an Offender

By Jay G. Heiser, Warren G. Kruse II

Nov 30, 2001

The Role of Computer Forensics in Stopping Executive Fraud

By Scott Laliberte, Ajay Gupta

Oct 1, 2004

[About](#) | [Legal Notice](#) | [Privacy Policy](#) | [Press](#) | [Jobs](#) | [Write For Us](#) | [Contact Us](#) | [Advertise](#) | [Site Map](#)

© 2006 Pearson Education, Addison-Wesley Professional. All rights reserved.
75 Arlington Street, Suite 300, Boston, MA 02116

informit network